UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,384	05/24/2001	Shingo Yamaguchi	203223US-28	1503

22850 7590 04/06/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 04/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/863,384	YAMAGUCHI, SHINGO	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *41-43,45,50-63,65 and 70-80* is/are pending in the application.

4a) Of the above claim(s) *1-40,44,46-49,64 and 66-69* is/are withdrawn from consideration.

5)☒ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *41-43,45,50-63,65 and 70-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 41-43, 45, 50-63, 65, and 70-80 are pending.

2. This is a Final rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 41-42, 50-62, and 70-80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flint, et al. (US 6,453, 419) and in further view of Wood, et al. (US 6,609, 198).

As per claim 41:

Flint, et al. discusses a method of controlling a network, comprising the steps of:

establishing a computer network connection between a computer **[COL.2, lines 30-42]** and an intermediate device which has network resources connected thereto; **[COL.3, lines 36-39]**

determining a level of security of the computer network connection **[COL.3, line 48 – COL.4, line 1]** based on determining whether the computer network connection to connect the computing device to the intermediate device is encrypted **[COL.4, lines 42-45]**, wherein the first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted; and **[COL.3, line 48 – COL.4, line 1 and COL.11, lines 58-59]**

controlling a level of access of the computing device to the network resources **[COL.4, lines 28-43 and COL.5, lines 1-4]** using the level of security of the computer network connection that has been determined **[COL.6, lines 7-10]**, such that the computing device is allowed access to a first set of network resources, including a file server, based on a determined first level of security, and is not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server **[COL.5, lines 39-40 and COL.12, lines 13-15]**, based on a determined second level of security **[COL.20, lines 53-67]**.

Flint teaches the system and method for implementing a security policy including a first and second region, one or more services bridging the first and second region, access control rules which defines a security policy wherein the access control rules limit data transfer by the one or more services bridging the first and second regions [COL.2, lines 15-28). Flint does teach determining the level of security and the controlling of the level of access according to the determined level when Flint discusses

the access rules which is applicant's level of security wherein the firewall (intermediate device) checks with the ACL's for the determined level of security which are the permissions and constraints [i.e. encryption requirements and authentication requirements) [COL.3, lines 48-60]. Further, Flint discusses the filter applies a condition to the connection where determining a level of security taught, the determining the communication protocol determines whether the computer network connection is encrypted [COL.3, line 48 – COL.4, line 1 and COL.11, lines 58-59]. The invention mainly concerns with the security of the connections [COL.2, lines 15-27] where rules are made and checks whether encryption is involved for the connections [COL.6, lines 6-10], thus, Flint does include different levels of security and that it is another (2^{nd}) level of security if it is checked and determined that there are no encryption for the particular connection [COL., lines 58-62]. The second level of security involves a different measure if there is no encryption than the first level of security if encryption were involved. The connection is checked to see if the connection is "true" when the connection meets the criteria and "false" branch if the connection does not meet the criteria [COL.4, lines 54-58]. The applying conditions to the connection and checking for authentication or encryption to determine the security of the connection is applicant's first and second security level [COL.4, lines 31-33 and 64-65]. The first security level is determined is true if checking and is determined that encryption is involved and the second level of security is false when it is checked and determined that the connection does not include encryption, therefore denies connection [COL.5, lines 38-43 and COL.6, lines 22-24].

However, the level of security was not further discussed in details of allowing access to the first set of network resources based on the determined first level of security and allowed access to the second set of network resources based on the second level of security.

Wood, et al. discloses an invention to better solve security issues addressed by isolating publicly accessible resources from more sensitive assets using the firewall techniques by having authentication schemes that are associated with trust level and environmental parameters [COL.2, lines 32-35]. Wood teaches the ability to upgrade credentials where a credential suitable for one resources in the initial resource set or requires authentication at higher trust level without the loss of session continuity whereby allows an entity to tailor its credentialing to current access requirements [COL.2, lines 51-63]. The level of security herein is discussed in the form of trust level which involves a first credential access to the first information resources and the second credential access to the second information resource [COL.3, lines 15-24] wherein individual types of access to a single resource have differing security requirements [COL.5, line 55 – COL.6, line 6].

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Flint to include allowing access to a first set of resources based on the first level of security and allowing access to a second set of resources based on the determined second level of security as taught by Wood [COL.8, lines 23-46], because this allows an entity to tailor its credentialing to current access requirements

and is more difficult to maintain a uniform security policy across a set of resources [COL.1, lines 58-62 and COL.2, lines 61-63].

As per claim 42: See Flint on COL.3, lines 33-39; discusses establishing a wireless computer network connection.

As per claim 44: Cancelled.

As per claims 46-49: Cancelled

As per claim 50: See Flint on COL.3, lines 47-53; discusses the step of determining is performed by the intermediate device, and said controlling is performed by the intermediate device.

As per claim 51: See Flint on COL.2, lines 15-20; discusses the step of determining is performed by the intermediate device which is a router.

As per claim 52: See Flint on COL.2, lines 15-20 and COL.3, lines 48-53; discusses the step of controlling is performed by the intermediate device which is a router having a firewall operation.

As per claim 53: See Flint on COL.2, lines 15-20 and COL.3, lines 33-39; discusses the step of establishing is performed using the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 54: See Flint on COL.3, lines 15-26 and COL.6, lines 22-24; discusses the step of determining is performed by a server running a network operating system, the server being different from the intermediate device, and the step of controlling is performed by the server running the network operating system.

As per claim 55: **See Flint on COL.3, lines 54-60;** discusses the step of determining is performed by the server which is running a network directory service.

As per claim 56: **See Flint on COL.2, lines 15-20;** discusses the step of establishing is performed by a bridge connected to the computer through the computer network connection.

As per claim 57: **See Flint on COL.2, lines 15-20 and COL.3, lines 33-39;** discusses the step of establishing is performed by the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 58: **See Flint on COL.3, lines 3-9 and 48-50;** discusses the level of access by a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 59: **See Flint on COL.11, lines 58-60;** discusses determining the level of security using the intermediate device.

As per claim 60: **See Flint on COL.3, lines 33-39;** establishing the computer network connection as a wireless connection using the intermediate device.

As per claim 61:

Flint, et al. discusses a method of controlling a network, comprising the steps of:

means for establishing a computer network connection between a computer **[COL.2, lines 30-42]** and an intermediate device which has network resources connected thereto; **[COL.3, lines 36-39]**

means for determining a level of security of the computer network connection **[COL.3, line 48 – COL.4, line 1]** based on determining whether the computer network connection to connect the computing device to the intermediate device is encrypted **[COL.4, lines 42-45]**, wherein the first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted; and **[COL.3, line 48 – COL.4, line 1 and COL.11, lines 58-59]**; and

means for controlling a level of access of the computing device to the network resources **[COL.4, lines 28-43 and COL.5, lines 1-4]** using the level of security of the computer network connection which that has been determined **[COL.6, lines 7-10]**, such that the computing device is only allowed access to a first set of network resources, including a file server **[COL.12, lines 14-15]**, based on a determined first level of security, and is not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server **[COL.5, lines 39-40 and COL.12, lines 12-13]**, based on a determined second level of security **[COL.20, lines 53-67]**..

Flint teaches the system and method for implementing a security policy including a first and second region, one or more services bridging the first and second region, access control rules which defines a security policy wherein the access control rules limit data transfer by the one or more services bridging the first and second regions [COL.2, lines 15-28). Flint does teach determining the level of security and the controlling of the level of access according to the determined level when Flint discusses

the access rules which is applicant's level of security wherein the firewall (intermediate device) checks with the ACL's for the determined level of security which are the permissions and constraints [i.e. encryption requirements and authentication requirements) [COL.3, lines 48-60]. Further, Flint discusses the filter applies a condition to the connection where determining a level of security taught, the determining the communication protocol determines whether the computer network connection is encrypted [COL.3, line 48 – COL.4, line 1 and COL.11, lines 58-59]. The invention mainly concerns with the security of the connections [COL.2, lines 15-27] where rules are made and checks whether encryption is involved for the connections [COL.6, lines 6-10], thus, Flint does include different levels of security and that it is another (2^{nd}) level of security if it is checked and determined that there are no encryption for the particular connection [COL., lines 58-62]. The second level of security involves a different measure if there is no encryption than the first level of security if encryption were involved. The connection is checked to see if the connection is "true" when the connection meets the criteria and "false" branch if the connection does not meet the criteria [COL.4, lines 54-58]. The applying conditions to the connection and checking for authentication or encryption to determine the security of the connection is applicant's first and second security level [COL.4, lines 31-33 and 64-65]. The first security level is determined is true if checking and is determined that encryption is involved and the second level of security is false when it is checked and determined that the connection does not include encryption, therefore denies connection [COL.5, lines 38-43 and COL.6, lines 22-24].

However, the level of security was not further discussed in details of allowing access to the first set of network resources based on the determined first level of security and allowed access to the second set of network resources based on the second level of security.

Wood, et al. discloses an invention to better solve security issues addressed by isolating publicly accessible resources from more sensitive assets using the firewall techniques by having authentication schemes that are associated with trust level and environmental parameters [COL.2, lines 32-35]. Wood teaches the ability to upgrade credentials where a credential suitable for one resources in the initial resource set or requires authentication at higher trust level without the loss of session continuity whereby allows an entity to tailor its credentialing to current access requirements [COL.2, lines 51-63]. The level of security herein is discussed in the form of trust level which involves a first credential access to the first information resources and the second credential access to the second information resource [COL.3, lines 15-24] wherein individual types of access to a single resource have differing security requirements [COL.5, line 55 – COL.6, line 6].

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Flint to include allowing access to a first set of resources based on the first level of security and allowing access to a second set of resources based on the determined second level of security as taught by Wood [COL.8, lines 23-46], because this allows an entity to tailor its credentialing to current access requirements

and is more difficult to maintain a uniform security policy across a set of resources [COL.1, lines 58-62 and COL.2, lines 61-63].

As per claim 62: See Flint on COL.3, lines 33-39; discusses means for establishing a wireless computer network connection.

As per claim 64: Cancelled.

As per claims 66-69: Cancelled.

As per claim 70: See Flint on COL.3, lines 15-25 and 54-57; discusses the means for determining is the intermediate device, and the means for controlling is the intermediate device.

As per claim 71: See Flint on COL.2, lines 15-20; discusses the means for determining is the intermediate device which is a router.

As per claim 72: See Flint on COL.2, lines 15-20 and COL.3, lines 48-53; discusses the means for controlling is the intermediate device which is a router having a firewall operation.

As per claim 73: See Flint on COL.2, lines 15-20 and COL.3, lines 33-39; discusses the means for establishing is the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 74: See Flint on COL.3, lines 15-26 and COL.6, lines 22-24; discusses the means for determining is a server running a network operating system, the server being different from the intermediate device, and the means for controlling is the server running the network operating system.

As per claim 75: **See Flint on COL.3, lines 54-60;** discusses the means for determining is the server which is running a network directory service.

As per claim 76: **See Flint on COL.2, lines 15-20;** discusses the means for establishing is a bridge connected to the computer through the computer network connection.

As per claim 77: **See Flint on COL.2, lines 15-20 and COL.3, lines 33-39;** discusses the means for establishing is the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 78: **See Flint on COL.3, lines 3-9 and 48-50;** discusses a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 79: **See Flint on COL.11, lines 58-60**discusses means for determining the level of security using the intermediate device.

As per claim 80: **See Flint on COL.3, lines 33-39;** discusses means for establishing the computer network connection as a wireless connection using the intermediate device.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 43, 45, 63, and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flint & Wood, and further in view of Microsoft Computer Dictionary, 5th Edition.

As per claim 43:

The Flint and Wood combination discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can be a wireless network connection **[Flint – COL.3, lines 17-39]**.

However, Flint fails to implicitly include the IEEE 802.11b standard and takes official notice of such standard.

According to the Microsoft Computer Dictionary, an IEEE 802.11 standard allows computers and other devices to communicate over a wireless network (see page 26). Therefore it would have been obvious for a person of ordinary skills in the art to include the IEEE 802.11b with the Flint and Wood combination because the computing devices

can communicate over a wireless network connection.

As per claim 45:

The Flint and Wood combination discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can be a wireless network connection **[Flint – COL.3, lines 17-39]**. However, Flint fails to imply the Wired Equivalent Privacy ("WEP") encryption method.

According to the Microsoft Computer Dictionary, WEP is an encryption standard algorithm system included as part of the IEEE 802.11 standard where shared secret key is used to encrypt packets prior to transmission between the wireless network devices and monitors packets in transit to detect attempts at modification (see page 565). Therefore it would have been obvious for a person of ordinary skills in the art to include WEP with the Flint and Wood combination because the transmission of packets is more secure by encrypting the packets and monitors the packets during transmission to detect any modification attempts.

As per claim 63:

The Flint and Wood combination discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can be a wireless network connection **[Flint – COL.3,**

lines 17-39]. However, Flint fails to implicitly include the IEEE 802.11b standard and takes official notice of such standard.

According to the Microsoft Computer Dictionary, WEP is an encryption standard algorithm system included as part of the IEEE 802.11 standard where shared secret key is used to encrypt packets prior to transmission between the wireless network devices and monitors packets in transit to detect attempts at modification (see page 565). Therefore it would have been obvious for a person of ordinary skills in the art to include WEP with the Flint and Wood combination because the transmission of packets is more secure by encrypting the packets and monitors the packets during transmission to detect any modification attempts.

As per claim 65:

The Flint and Wood combination discusses establishing computer network connection between a computing device and a firewall that has network resources connected thereto wherein the firewall controls communications between networks and the Virtual Private Network which can be a wireless network connection **[Flint – COL.3, lines 17-39]**. However, Flint fails to imply the Wired Equivalent Privacy ("WEP") encryption method.

According to the Microsoft Computer Dictionary, WEP is an encryption standard algorithm system included as part of the IEEE 802.11 standard where shared secret key is used to encrypt packets prior to transmission between the wireless network devices and monitors packets in transit to detect attempts at modification (see page 565). Therefore it would have been obvious for a person of ordinary skills in the art to include

WEP with the Flint and Wood combination because the transmission of packets is more secure by encrypting the packets and monitors the packets during transmission to detect any modification attempts.

Response to Arguments

5. Applicant's arguments with respect to claims 41-80 have been considered but are moot in view of the new ground(s) of rejection.

The invention mainly concerns with the security of the connections [COL.2, lines 15-27] where rules are made and checks whether encryption is involved for the connections [COL.6, lines 6-10], thus, Flint does include different levels of security and that it is another (2^{nd}) level of security if it is checked and determined that there are no encryption for the particular connection [COL., lines 58-62]. The second level of security involves a different measure if there is no encryption than the first level of security if encryption were involved. The connection is checked to see if the connection is "true" when the connection meets the criteria and "false" branch if the connection does not meet the criteria [COL.4, lines 54-58]. The applying conditions to the connection and checking for authentication or encryption to determine the security of

the connection is applicant's first and second security level [COL.4, lines 31-33 and 64-65]. The first security level is determined is true if checking and is determined that encryption is involved and the second level of security is false when it is checked and determined that the connection does not include encryption, therefore denies connection [COL.5, lines 38-43 and COL.6, lines 22-24].

Flint's access rules are referring to applicant's level of security. Flint does teach determining the level of security and the controlling of the level of access according to the determined level when Flint discusses the access rules wherein the firewall (intermediate device) checks with the ACL's for the determined level of security which are the permissions and constraints [i.e. encryption requirements and authentication requirements) [COL.3, lines 48-60]. Further, Flint indicates for each connection attempt, the firewall checks the access rules against the defined access rules which are against the ACL's and encryption requirements can be part of the lists of constraints or permissions. A requirement is a condition where there may be a need or may not be a need. Thus, encryption requirements as discussed in Flint is whether there is a need for encryption or a condition that an encryption is not necessary.

Although, Flint discusses the access control rules which defines a security policy for the first and second regions, but did not fully go further of discussing having the distinct levels of security such first security level for one set of resources and another security level for second set of resources. Thus, the examiner has brought forth the Flint and Wood combination to teach this limitation.

The trust level as taught by Wood is applicant's level of security. Wood indicates that a uniform security policy across a set of resources is more difficult to maintain. Thus, Wood allows an entity to tailor its credentialing to current access requirements [COL.2, lines 51-63] wherein involves a first credential access to the first information resources and the second credential access to the second information resource [COL.3, lines 15-24] wherein individual types of access to a single resource have differing security requirements [COL.5, line 55 – COL.6, line 6].

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Flint to include allowing access to a first set of resources based on the first level of security and allowing access to a second set of resources based on the determined second level of security as taught by Wood [COL.8, lines 23-46], because this allows an entity to tailor its credentialing to current access requirements and is more difficult to maintain a uniform security policy across a set of resources [COL.1, lines 58-62 and COL.2, lines 61-63].

Conclusion

6 THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

HOSUK SONG
PRIMARY EXAMINER